IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

COMMUNITY BANK OF TRENTON, UNIVERSITY OF ILLINOIS EMPLOYEES CREDIT UNION, FIRST FEDERAL SAVINGS BANK OF CHAMPAIGN-URBANA, and SOUTHPOINTE CREDIT UNION, individually and on behalf of all similarly situated payment card issues,	)	
Plaintiff,	)	
vs.	)	**Case No. 15-cv-01125-MJR**
SCHNUCK MARKETS, INC.,	)	
Defendant.	)	

MEMORANDUM AND ORDER

REAGAN, Chief District Judge:

A. Introduction and Procedural Overview

This case is now before the Court on the Plaintiffs' Amended Complaint and the Defendant's Motion to Dismiss (Docs. 52, 55). The underlying dispute concerns a data breach at Defendant's grocery stores between December 2012 and March 2013. The initial complaint identified two grounds for federal jurisdiction—18 U.S.C. § 1961, et seq., pursuant to 18 U.S.C. § 1964(a) & (c) ("Racketeer Influenced and Corrupt Organizations Act" aka "RICO"); and 28 U.S.C. § 1332(d) ("Class Action Fairness Act" aka "CAFA"). The Amended Complaint contains no RICO claims, so the sole remaining jurisdictional basis is CAFA. The Motion to Dismiss

having been fully briefed, the Court now finds that Plaintiffs have failed to state a plausible claim for relief.

This Court accepts all factual allegations as true when reviewing a 12(b)(6) motion to dismiss. ***Erickson v. Pardus*, 551 U.S. 89, 94 (2007).** To avoid dismissal for failure to state a claim, a complaint must contain a short and plain statement of the claim sufficient to show entitlement to relief and to notify the defendant of the allegations made against him. **FED. R. CIV. P. 8(a)(2); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555-57 (2007).** In order to meet this standard, a complaint must describe the claims in sufficient factual detail to suggest a right to relief beyond a speculative level. ***Id.; Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); *EEOC v. Concentra Health Servs.*, 496 F.3d 773, 776 (7th Cir. 2007).** A complaint need not contain detailed factual allegations, ***Scott v. Chuhak & Tescon, P.C.*, 725 F.3d 772, 782 (7th Cir. 2013)**, but it must go beyond "mere labels and conclusions" and contain "enough to raise the right to relief above the speculative level," ***G&S Holdings, LLC v. Cont'l Cas. Co.*, 697 F.3d 534, 537-38 (7th Cir. 2012).**

The Seventh Circuit has outlined the boundaries of 12(b)(6) with two major principles. First, that although facts in the pleadings must be accepted as true and construed in the plaintiff's favor, allegations in the form of legal conclusions are insufficient to survive a motion to dismiss. ***McReynolds v. Merrill Lynch & Co., Inc.*, 694 F.3d 873, 885 (7th Cir. 2012).** And, second, "the plausibility standard calls for 'context-specific' inquiry that requires the court 'to draw on its judicial experience and common sense.'" ***Id.*** Threadbare recitals of elements and conclusory statements are not sufficient to state a claim. ***Id.*** Put another way, to survive a motion to dismiss "the plaintiff must give enough details about the subject-matter of the case to present a

story that holds together [. . .] the court will ask itself *could* these things have happened, not *did* they happen." ***Swanson v. Citibank, N.A.*, 614 F.3d 400, 404 (7th Cir. 2010).**

The case before the Court now presents 7 different theories of relief—down from 13 in the initial complaint. As was outlined in this Court's ruling on the initial complaint and initial motion to dismiss, many of the theories have been tested in other data breach litigation against major retailers across the country, such as Target, Jimmy Johns, Barnes and Noble, Home Depot, and Neiman Marcus, to name a few.[1] The initial complaint was dismissed by this Court in large part because it suffered from vast generalizations. The Amended Complaint and pleadings now before the Court have attempted to shore up the problem of generality, doing so in part by narrowing the scope of issues before the Court by removing the RICO and fraud claims, and omitting claims the Court previously dismissed. The additional facts that have been brought forth will be recited below. The Court will then provide a detailed legal analysis of the Amended Complaint.

However, as a preliminary matter, the Court must address jurisdiction. The Amended Complaint alleges that this Court has subject matter jurisdiction under CAFA. At an earlier point in the proceedings, the Plaintiffs had filed a motion for class certification (Doc. 12), which they voluntarily withdrew, with the opportunity to refile it later without prejudice (Dkt. txt

[1] *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016) (customer suit reversed and remanded after standing found appropriate); *Irwin v. Jimmy John's Franchise, LLC*, 2016 WL 1355570 (C.D. Ill. 2016) (customer suit with certain claims under Illinois law dismissed); *In re Home Depot, Inc., Customer Data Security Breach Litigation*, 2016 WL 2897520 (N.D. Ga. 2016) (customer suit involving 56 million customers allowed to proceed on certain claims beyond motion to dismiss); *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015) (customer suit, standing found to be proper); *In re Target Corp. Data Sec. Breach Litigation*, 66 F.Supp.3d 1154 (Minn. D. Ct. 2014) (customer suit dismissed as to some claims, allowed to proceed as to others); *In re Barnes & Noble Pin Pad Litigation*, 2013 WL 4759588 (N.D. Ill. 2013) (customer suit dismissed on standing grounds).

entry 42). Though the Plaintiffs have not refiled their motion for class certification, in part due to this Court's direction that it was not necessary to do so at this point (*See* Dkt. txt. entry 60 (granting Plaintiffs' unopposed motion for an extension of time to file a class certification motion until after the motion to dismiss was ruled upon), the Court nevertheless finds that it has jurisdiction under CAFA prior to formal class certification. ***See Greenberger v. GEICO General Ins. Co.*, 631 F.3d 392, 396 (7th Cir. 2011) ("federal jurisdiction under CAFA does not depend on class certification").**

B. <u>Factual Allegations</u>

Many of the facts in the Amended Complaint are identical to those offered in the original complaint. Of new vintage, the Plaintiffs allege that they were intended or third-party beneficiaries to the contracts between the Defendant and others in the card processing network because Plaintiffs received an interchange fee or interest for processing cards. (Doc. 52 at 10-11). Plaintiffs also included allegations that Defendant has yet to upgrade to more secure transaction chip technology to allow customers to pay more safely (*Id.* at 10).

Plaintiffs' Amended Complaint presented specific figures about the scope of the data breach—including that unencrypted data was potentially compromised for 2.4 million cards swiped at 79 Schnucks' stores from December 1, 2012 through March 30, 2013 (Doc. 52 at 15). The complaint also contained the allegation that stolen data was used in fraudulent transactions across the globe, evidencing that it was unencrypted and improperly stored (*Id.* at 29). On March 14, 2013, Defendant first learned of a data breach upon receiving reports of fraudulent card use (*Id.* at 20). On March 19 it retained Mandiant, a forensic investigation firm, to investigate the issue (*Id.*). Mandiant took action, identifying the infirmity on March 20 (*Id.*).

However, Defendant did not inform the public of the issue until March 30, 2013, at which time the issue was fully contained (*Id.*). By their calculations, Plaintiffs allege that the gap from March 19 through March 30th allowed an unnecessary window for the compromise of 340,000 payment cards, assuming a rate of 20,000 cards used per day (*Id.* at 21-22). Plaintiffs allege that Defendant did not pursue a reasonable alternative by posting a "cash or checks only" sign specifically because it knew it would be bad for business (*Id.* at 22).

C. Legal Analysis

1. Negligence/gross negligence – Missouri law only

Under Missouri law, to establish a claim for negligence a plaintiff must prove: "a (1) legal duty on part of the defendant to conform to a certain standard of conduct to protect others against unreasonable risks; (2) a breach of that duty; (3) a proximate cause between the conduct and the resulting injury; and, (4) actual damages to the claimant's person or property**."** ***Hoover's Dairy, Inc. v. Mid-America Dairymen, Inc. Special Products, Inc.*****, 700 S.W.2d 426, 431 (Mo. 1985).** As both parties acknowledge, Missouri law requires notification in the event of a data breach—pursuant to MO. REV. STAT. § 407.1500—Missouri's data breach notification law. However, the data breach notification statute exclusively bestows the power to prosecute violations upon the Missouri Attorney General. ***See*** **MO REV. STAT. § 407.1500.4.** What is more, the statute does not contemplate a duty or remedies for anything other than a failure to notify. This Court will not read additional duties into a law carefully crafted by the legislature, particularly where the legislatures of other states have explicitly contemplated additional protections in legislation. ***Compare*** **MO. REV. STAT. § 407.1500.4** ***with*** **MINN. STAT. § 325E.64 (Plastic Card Security Act).** Reading the statute as a whole, this means that in Missouri the

only statutory duty regarding data security is to provide notice of a breach, and the only authority to prosecute a failure of this duty is the attorney general.

Statutory duties aside, the Plaintiffs also argue that the Defendant had a duty to safeguard data based on its business relationship; sound public policy; industry standards; best practices; or implied contracts. In support of these arguments, Plaintiffs rely heavily on out-of-circuit precedent from Georgia, Minnesota, and Pennsylvania. ***See Home* Depot, 2016 WL 2897520; Target, 64 F.Supp.3d at 1309-1310; *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 395 F. Supp.2d 183, 193-96 (M.D. Penn. 2005) (finding a common law duty on behalf of a retailer to an issuing bank based on social policy, the business relationship, and the foreseeability of harm); *First Choice Federal Credit Union v. The Wendy's Co.*, 2:16-cv-NBF-MPK (W.D. Pa. Feb. 13, 2017) (Doc. 80) (report and recommendation denying motion to dismiss a financial institution's negligence claim in a data breach case)[2].** The out-of-circuit precedent is distinguishable from the present case.

First, as to the Georgia precedent in the *Home Depot* data breach litigation, this precedent does not give rise to a negligence claim under Missouri law because that litigation is factually distinct, and in a subsequent opinion, a Georgia appellate court disagreed with the Northern District of Georgia's interpretation of Georgia law. ***See Home Depot*, 2016 WL 2897520 at *1-2, *but cf McConnell v. Dept. of Labor*, 787 S.E.2d 794, 798-800, n.4 (Ga. Ct. App. 2016).** The Home Depot case is factually distinct because the facts in the record suggest that Home Depot's data security conduct in the lead up to their breach was egregious and intentional—Home Depot on

[2] This report and recommendation allows negligence claims to proceed beyond a motion to dismiss without citing any authority for or against the recommendation. What is more, the recommendation acknowledges the potential latent issues regarding choice of law, etc. that may ultimately weigh on the appropriateness of a negligence claim.

numerous occasions ignored warning signs of poor data security, and even went so far as to fire tech employees who tried to alert the company to the risks of the poor data security measures. ***See Home Depot*, 2016 WL 2897520 at *1-2.** Such alarming conduct certainly weighed heavily on the Northern District of Georgia when deciding whether or not to let a negligence claim proceed. In allowing the claim to proceed, the *Home Depot* Court explicitly called upon a proposition of Georgia law, that there is a "general duty one owes to all of the world not to subject them to an unreasonable risk of harm." ***See id.* at *3**. But subsequent to the *Home Depot* Court's holding, the Georgia Court of Appeals lamented such a broad interpretation of that 'general duty' and indicated that Georgia courts would not be bound by a federal court's interpretation of Georgia law. ***See McConnell*, 787 S.E.2d at 798-800, n.4 (declining to recognize a general duty or a theory of negligence in a suit by an employee regarding an employer's data security practices over employee data)**. The *McConnell* Court's analysis emphasized the egregious nature of Home Depot's conduct in declining to allow a negligence claim to proceed regarding data security of an employee's personal information. ***See id.* at 798-800, n.4.** Based on these distinctions, this Court is not persuaded that it should follow the *Home Depot* Court in recognizing a duty here.

Second, as to the *Target* precedent, this Court does not find the duty recognized in that litigation to play a role in this case because the *Target* Court relied in part upon data security provisions unique to Minnesota law—provisions which have no analogue in Missouri law. ***See In re Target Corp. Customer Data Sec. Breach Litigation*, 64 F.Supp.3d at 1310, 1312-13 (noting Minnesota's policy of punishing companies that do not secure customer data); MINN. STAT. § 325E.64 (Plastic Card Security Act).** As was noted above, the Missouri legislature has not

crafted such particularized data security legislation. In the absence such legislation, this Court declines to *sua sponte* create a duty where the Missouri government has declined to do so.

Third, as to the Pennsylvania precedent cited by Plaintiffs, this Court finds the precedent unpersuasive because the *BJ's* case is frankly outdated, and the other case cited has no authoritative force whatsoever as a contested report and recommendation. ***See Sovereign Bank v. BJ's Wholesale Club, Inc.*, 395 F.Supp.2d at 193-95 (assessing potential elements of negligence and concluding that the negligence claim could proceed beyond the motion to dismiss).** The *BJ's* case was decided in 2005, prior to the onslaught of data breaches and litigation, and prior to the time when many legislatures began considering the issue of data security legislation. ***Id.*** Missouri's own data security legislation post-dates *BJ's*. ***See* MO. REV. STAT. § 407.1500 (enacted in 2009).** Thus, the Court will not rely on such old precedent to acknowledge a duty in a rapidly changing area of law.

Precedent aside, the Court is not persuaded that public policy concerns, the existence of industry standards, or implied contractual relationships should give rise to a duty in this case. The parties squabble over their respective levels of sophistication, the foreseeability of data security risks, and the best ways to address losses incurred in the aftermath of a breach. The breach at Defendant's stores took place during what seemed to be the boom of data breach activity, at a time when many retailers were caught either unaware or unluckily in the cross-hairs of cybercrime. Unfortunately losses were sustained, losses that in retrospect should have or could have been prevented, but not every loss can be compensated via legal action. In the wake of the data breach boom, it seems fair to say retailers will have to act more prudently, but

at the time that this breach occurred the law did not contemplate harms of the kind that emerged.[3]

Finally, as to the theory that Section 5 of the Federal Trade Commission (FTC) Act gives rise to a duty and negligence, the Court previously declined this argument under Illinois law, and hereby extends that rational to claims under Missouri law (*See* Doc. 50 at 25-26). The sole power to enforce the FTC rests with the Commission, and there is no private cause of action. ***See e.g. Baum v. Great Western Cities, Inc. of New Mexico*, 703 F.2d 1197, 1209 (10th Cir. 1983); *Meyer v. Bell & Howell Co.*, 453 F.Supp. 801, 802 (E.D. Mo. 1978).** In sum, the Court finds that under Missouri law the Defendant had no duty to protect customer information on the Plaintiffs' behalf.

2. <u>Negligence *per se* – Missouri law only</u>

This Court dismissed the negligence *per se* claim from the original complaint after finding that Plaintiffs had failed to identify a duty the Defendant violated. (Doc. 50 at 27-28). Here, the Court will do the same.

3. <u>Breach of implied contract—Missouri law, or for subclass in Missouri and Illinois</u>

Under Missouri and Illinois law an implied contract is created by the parties' conduct and must contain all of the elements of a traditional contract, including offer, acceptance, consideration, and a meeting of the minds. ***See C. Szabo Contracting Inc. v. Lorig Constr. Co.*, 19 N.E.3d 638, 644 (Ill. App. Ct. 2014); *Kosher Zion Sausage Co. of Chicago v. Roodman's, Inc.*, 442 S.W.2d 543, 546 (Mo. Ct. App. 1969).**

[3] It is interesting to note that the breach at Defendant's stores came before the breach at Target (December 2013), and before the breach at Home Depot (2014). This timeline weighs against finding that the litigation or conduct in either of those breaches should have put Defendant on heightened notice or imposed a stricter duty for Defendant to monitor data security.

Plaintiffs' theory of implied contract in the amended complaint relies heavily upon the assertion that Plaintiffs authorized transactions on the "implicit promise" that Defendant had adequate data security measures. As consideration for this exchange, Plaintiffs assert that they got interchange fees and Defendant got payment for the goods purchased by Plaintiffs' customers. Plaintiffs urge that absent the "implicit promise" of a secure data network, they would have refused to authorize payments, advised their customers to shop elsewhere, canceled and reissued compromised cards, and taken other cost-saving or protective measures. These assertions are in large part a repeat of what was set forth in the original complaint, although the facts have been enhanced somewhat by the scarce details about interchange fees as consideration. ***See Egan v. St. Anthony's Medical Ctr.*, 244 S.W.3d 169, 174 (Mo. 2008) (finding that a preexisting duty cannot furnish consideration for a contract).** Other parties (Defendant, Defendant's banks, VISA, and Mastercard) had explicit contracts and duties to each other, so this Court will not stretch those preexisting relationships and agreements to impliedly include Plaintiffs.

In the first instance, this Court dismissed the theory of implied contract because the Plaintiffs had failed to make out the essential elements of a contract—offer, exchange, and acceptance. Here, the Court finds that the implied contract theory continues to suffer from this infirmity. It is still not clear what 'contract' was made between *these* parties, or how there was a direct violation of said relationship. The implied contract theory seems to bleed over into the theory of third-party beneficiary because the Plaintiffs repeatedly allege that the Defendant was required to maintain proper data security per its agreements with VISA and MasterCard, but the parties have not cited any portion of those contracts that expressly or impliedly

contemplates the alleged relationship Plaintiffs now rely upon. Under Missouri law this is particularly problematic because Missouri law will not imply a contract where there is a pre-existing relationship.

The allegations that Plaintiffs would have withheld authorization or taken other protective measures are irrelevant to the issue of an implied contract because these things do not bear on the offer-acceptance-consideration trio, or if they do, they do not relate in a way that feasibly could have prevented a breach. A financial institution's decision to decline authorization, thereby declining acceptance, does not prevent a data breach because the data has already been gathered by the Defendant at that time—so declining 'acceptance' of the transaction offers no protection of the sort sought under the theory of implied contract. Withholding authorization or canceling compromised cards are steps that the Plaintiffs could have and perhaps did take after the breach became apparent to mitigate harms, but these things are extraneous to the formation of an implied contract in the first instance.

Once again, the Plaintiffs reference the term 'implied in law' contract, but they offer little factual or legal argument on the matter. Instead, they point to the unjust enrichment count of their complaint, where the argument focuses primarily on unjust enrichment. An 'implied in law' contract has elements distinct from an implied in fact contract, so without any argument or factual allegations this Court will not allow this count to proceed under the guise of that legal theory.

4. **Breach of contracts to which Plaintiffs are third-party beneficiaries**

Under either Illinois or Missouri law, the showing required to establish third-party beneficiary status to a contract is relatively high. The primary component under the laws of

both states is that the party claiming third-party status must be able to show that they are more than an incidental or happenstance beneficiary. Under Illinois law a party must make a significant showing about their status as an intended beneficiary to a contract before a court will recognize such a relationship. ***See e.g. Bank of Am. Nat. Ass'n v. Bassman FBT, L.L.C.*, 981 N.E.2d 1, 11 (Ill. App. Ct. 2012) ("That the parties expect, know, or even intend that the contract benefit others is insufficient to overcome the presumption that the contract was intended only for the parties' *direct* benefit."); *Kansas City Hispanic Ass'n Contractors Enterprise, Inc. v. City of Kansas City*, 279 S.W.3d 551, 555 (Mo. Ct. App. 2009).** To be recognized as a third-party beneficiary, Plaintiffs must identify an express portion of a contract that contemplates their status as a beneficiary.

On the record before the Court, the Court does not find that there are sufficient factual allegations that the Plaintiffs were intended third-party beneficiaries of any contracts between the Defendant and other participants in the card network. It is not at all clear how the ability of a cardholder to use a card at a merchant, or the use of intermediaries to facilitate this process could be interpreted to *directly* benefit the Plaintiffs. Plaintiffs do allege in the Amended Complaint that they get an interchange fee or interest related to each customer transaction, but this peripheral benefit does not support the assertion that they were intended to directly enforce or otherwise control the contractual relationship between the merchant and the card processing network. Absent these allegations, the Court dismisses this claim because it does not find that the facts presented are sufficient to state a plausible claim.

5. Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act

"To state a violation of the [Consumer Fraud Act], the plaintiffs must prove three elements: (1) an unfair or deceptive act or practice by the defendant; (2) the defendant's intent that plaintiff rely on the deception; and, (3) the occurrence of the deception in the course of conduct involving trade or commerce." ***Parks v. Wells Fargo Home Mortgage, Inc.*, 398 F.3d 937, 943 (7th Cir. 2005).** Like any fraud claim in Illinois, a plaintiff must plead a consumer fraud claim with particularity by alleging the identity of the person who made the misrepresentation, the time, place, and content of the misrepresentation, and the method by which the misrepresentation was communicated. ***Bankers Trust Co. v. Old Republic Ins. Co.*, 959 F.2d 677, 683-84 (7th Cir. 1992).** Though there may be flexibility in the pleading standard where the plaintiffs allege that they do not have access to the information needed to show a fraud, the flexibility is not so great that plaintiffs can satisfy the particularity requirement by simply asserting that on "information and belief" the defendants committed consumer fraud**.** ***Id.***

Aside from specific claims of fraud or deception, Illinois courts also allow general claims that certain conduct is unfair or deceptive. ***See e.g. Wendorf v. Landers*, 755 F.Supp.2d 972, 978-79 (N.D. Ill. 2010).** Such a claim is subject to a multi-part test: "(1) whether the practice offends public policy; (2) whether it is immoral, unethical, oppressive, or unscrupulous; [and] (3) whether it causes substantial injury to consumers." ***FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 244, n.5 (1972).** Illinois courts have held that a claim need not fulfill all three factors. ***See Robinson v. Toyota Motor Credit Corp.*, 775 N.E.2d 951, 961 (Ill. Sup. 2002).** "To constitute an unfair practice, the defendant's conduct must violate public policy, be so oppressive that it leaves the consumer with little alternative except to submit to it, and injure the consumer."

Rockford Memorial Hosp. v. Havrilesko*, 858 N.E.2d 56, 65 (Ill. App. 2d Dist. 2006).** Such a claim must still be pled with sufficient particularity. ***See Demitro v. General Motors Acceptance Corp.*, 902 N.E.2d 1163, 1168-70 (Ill. App. Ct. 1st Dist. 2009).** In *Demitro* an Illinois appellate court found that an automobile lender's conduct was oppressive where the conduct effectively gave a leasee the choice of paying more than $39,000 within a few weeks' notice, or face permanent repossession of his vehicle, rather than allowing him to pay just over two-thousand dollars to remedy a default on his payments. ***Id. The *Demitro* Court was particularly sensitive to the "oppressive" impact of the lending company prematurely repossessing the vehicle, despite letters and conversations suggesting plaintiff had more time to remedy his default**.** ***Id.***

Research did not reveal a published decision where an Illinois Court considered a data breach incident at a merchant. Most similar was a case where an Illinois appellate court considered a data breach in the context of theft of medical records. ***See Maglio v. Advocate Health and Hospitals Corp.*, 40 N.E.3d 746 (Ill. App. Ct. 2d Dist. 2015) (affirming dismissal of plaintiff-patients' data breach suit against health care provider based on finding that plaintiffs did not suffer actual injury and thus lacked standing).** Also similar was a case where an Illinois appellate court considered the risk of a security breach at an ATM machine. ***See Popp v. Cash Station, Inc.*, 613 N.E.2d 1150 (Ill. App. Ct. 1st Dist. 1992) (finding that plaintiff cash machine customers failed to plead a sufficiently particular misrepresentation or fraud where they did not identify a statement or misrepresentation made to them about cash machine security).** Neither of these cases lends traction to Plaintiffs' claims in the matter before the Court.

Interpreting ICFA, the Seventh Circuit held that an unfair or deceptive practice claim must be based on more than a simple breach of contract. ***Greenberger*, 631 F.3d at 399-400.**

In their initial complaint, Plaintiffs pursued a claim under ICFA on the premise that Defendant made an unfair, false, or fraudulent misrepresentation about their data security practices. The claim invoked the particularity pleading standard, and this Court dismissed the claim because it was not clear what misrepresentation or fraudulent statement was made and relied upon. (*See* Doc. 50 at 32-33). Rather than clarifying their original claim to identify a particular misrepresentation, Plaintiffs Amended Complaint contains an ICFA claim centered on the theory that Defendant participated in an unfair practice by failing to maintain adequate data security. Defendant retorted that Plaintiffs' claim could not succeed because Plaintiffs failed to allege that the consumers were harmed by the unfairness.

Plaintiffs put significant weight on the *Home Depot* Court's finding that financial institutions could maintain a claim against that retailer under ICFA. However, as was previously discussed, the *Home Depot* opinion appears to be an outlier, and was based on facts indicating egregious conduct by the retailer. Thus, the conduct by Home Depot might arguable have risen to the level of oppressive conduct. *Home Depot* aside, the Court finds Plaintiffs' factual and legal allegations to be too threadbare to suggest a plausible theory of relief.

The Court does not find a concrete public policy that has been violated. Defendant was not explicitly advertising data security or luring customers into the store on the premise that it practiced better data security than other retailers, nor were issuing banks being lured into authorizing transactions on the basis that Defendant's data security was top notch. Though there might have been a general market expectation that any retailer would practice prudent

data security, the facts do not suggest that Defendant gamed the market to take advantage of consumers of financial institutions on these grounds. The Plaintiffs' complaint also lacks any suggestion of oppressive conduct. Unlike Home Depot's conduct of skirting warnings and firing employees, Defendant retained a firm to investigate a potential breach within a day of learning of it. Finally, as to the requirement that consumers be injured, it is noteworthy that the *consumers* were apparently reimbursed for the trouble caused by the breach, so there is a possibility that Plaintiffs' claim would also fail on this basis. Accordingly, this count is dismissed.

6. <u>Unjust enrichment/assumpit</u>

The Court dismissed the unjust enrichment/assumpit claims in its review of the original complaint because it found that Defendant did not retain an added bonus from customers shopping with a card as opposed to those shopping with cash. (Doc. 50 at 33-35). The only alteration to the arguments on this claim in the Amended Complaint is that Plaintiffs now argue there was unjust enrichment from March 14 to March 30, the date Defendant learned of a potential breach until the date it was locked down and announced to the public. However, the Court does not find this narrower range to remedy the defect it identified earlier with this claim—shoppers still did not pay more for groceries via card than they would have with cash, so it cannot be said Defendant made more than it should have for those particular groceries. Accordingly, this Count is dismissed for the same reasons set forth in this Court's initial dismissal. (Doc. 50 at 33-35).

7. Declaratory and injunctive relief

The Court will not comment on the propriety of the relief sought because it is dismissing the substantive claims in the Complaint.

8. Conclusion

For the foregoing reasons, the Court **GRANTS** Schnucks's Motion to Dismiss (Doc.[55]): all counts are dismissed with prejudice because the Court is of the opinion that further amendments will not present a plausible theory for relief.

IT IS SO ORDERED.

DATED: May 1, 2017

s/ Michael J. Reagan
MICHAEL J. REAGAN
Chief Judge
United States District Court